Statement

Of

Kenneth J. Dunlap

Director, Security North America

International Air Transport Association (IATA)

"An Assessment of Checkpoint Security: Are Our Airports Keeping Passengers Safe?"

Before the

U.S. House of Representatives

Committee on Homeland Security

Subcommittee on

Transportation Security and

Infrastructure Protection

March 17, 2010

Introduction

Chairwoman Jackson-Lee, Ranking Member Dent, and distinguished Members of the Subcommittee, thank you for the opportunity to testify at this hearing: "An Assessment of Checkpoint Security: Are Our Airports Keeping Passengers Safe?" The International Air Transport Association (IATA) appreciates the leadership and the foresight of the Subcommittee in addressing this critical issue in the wake of the attempted bombing on Christmas Day. It is my hope that today's hearing launches a much needed international dialog on the future of passenger screening and results in even better screening for this generation and the next. I urge you and your colleagues to seize this opportunity.

IATA represents some 230 US and foreign air carriers and has offices in over 70 countries. IATA's mission is to promote safe and secure air travel. Through our work, we have changed the way people fly around the globe. In fact, your last trip across the United States or across an ocean was touched by IATA. The airline on which you flew most likely participated in the IATA Operational Safety Audit (IOSA). This is an internationally recognized and accepted evaluation system designed to assess the operational management and control systems of an airline. IATA replaced paper tickets with etickets which allow you to fly using just your identification and a boarding pass. IATA has enabled passengers to check in at home and to use boarding passes displayed on a Blackberry or PDA through our standard setting processes and committees.

These initiatives embody one of IATA's core competencies, which is to develop the processes that help passengers and their bags move through airports more efficiently. Through IATA's flagship programs, Simplifying the Business (StB) and Fast Travel, we work to make passenger travel through the aviation system faster and simpler. Through our work in areas such as boarding pass encryption and checkpoint entry lanes, we work to make travel more secure. This experience serves as the foundation for the ideas we are presenting to you this afternoon.

IATA's Vision of the Future.

IATA has a vision of future passenger screening that is based on a paradigm shift in the principals behind checkpoint operation. We believe next generation checkpoints must focus on looking for "bad people" and not just "bad things." If we have learned anything from the last decade, it is that a passenger with toe nail clippers is not automatically a threat to aviation.

As the Subcommittee reviews the events post-December 25th, we expect many may seek short-term fixes to security checkpoints. In fact, some procedural changes may be warranted. However, simply dropping new technology into a checkpoint is not the answer for the future and does not guarantee improved security. Even the best technology cannot detect bad people. This Congress cannot allow calls for new equipment to mask the fact that a long-term change is required for security checkpoints.

Consider our vision of an effective checkpoint, which focuses on looking for bad people rather than for bad things:

> Passengers are treated with dignity. Babies and children sharing a name found on the no fly-list pass through screening uneventfully. Toe nail scissors and nail clippers do not trigger an interrogation.

In this scenario, the checkpoint is no longer the first line of defense, but a second look. The dots are connected by intelligence agencies before passengers reach the checkpoints, plots are disrupted long before the airport, and screeners look for behavioral clues warranting a closer inspection of the passenger.

IATA believes the key to this future lies in leveraging all of the passenger information currently collected by a government before the start of the trip. Data collected in the name of customs and immigration needs to be merged with data collected for security. Then this comprehensive data should be analyzed by government intelligence agencies before a "cleared to board" decision is issued. The general results of this vetting should be made known to the screener at the checkpoint who

will decide if a more thorough physical search is warranted. This process, combined with advanced behavior detection, would make for a stronger and more efficient checkpoint.

Certainly, all the parts of this notional checkpoint exist today. However, government and industry need to work together to integrate these elements into a single, useable process. We believe Congress should make this integration a priority.

Today's Department of Homeland Security (DHS)

IATA applauds Secretary Napolitano, Chairman Thompson, and Chairwoman Jackson-Lee for refocusing DHS to a more forward-thinking and globally-oriented Department. There are no better examples than IATA's testimony today and Secretary Napolitano's joint Global Security Summit in Geneva with IATA. The industry has noticed this new approach and looks to heightened engagement to make the checkpoint of the future a reality.

Recommendations to Congress and to the Department of Homeland Security

During our Summit, IATA offered five principles and recommendations to DHS to guide commercial aviation security post-Christmas day. We believe these guidelines apply both locally and also globally. Our five principles include:

1. Define a risk based approach

Aviation security resources in terms of people and funds are limited. Regulators and industry must focus these on the most probable threats to aviation as demonstrated by past threats and future capabilities. This requires that industry and government work in partnership to identify and to prioritize the threats we expect to face and the responses we expect to implement.

2. Act globally

Aviation is a globally interconnected enterprise that supports 32 million jobs and $3.5 trillion dollars in economic activity.[1] As such, this global network will only be as strong as its weakest link. Regulators must secure this system with internationally implemented standards and recognize the comparable security measures of other states. Security resources should not be wasted duplicating the efforts of other competent regulators.

3. Regulators must share and be open to best practices

Globally, air transport is more secure than ever in its history. IATA applauds the many states that have raised the bar on their security programs. However, we often see the "not invented here" mentality preventing wider adoption of new and innovative security methods. IATA encourages states to use the International Civil Aviation Organization (ICAO) more effectively on security to develop harmonized security policies and to spread best practices.

4. Work with industry on practical solutions

The best security is based on procedures and equipment that work in concert with the complex operating environment within which global aviation operates. IATA urges regulators to tap into industry experience and expertise to deploy efficient and effective security measures.

5. Act Strategically

Security incidents should not be met with reactive and unilateral government actions. Often, the most ineffective measures are written immediately following a security breach. Industry and government must focus on making existing processes and resources even more effective. At the same time we must not be afraid to look at the whole system when we have evidence and technology to support generational change to meet new threats.

[1] IATA Economics 2010

Certainly, these are high level principles, but they must form the cornerstone of aviation security policy and be supplemented with specific recommendations. To that end, IATA provided Secretary Napolitano with five specific recommendations to strengthen security in the future. These are addressed to DHS and TSA, but should serve as the foundation for the efforts of other regulators as well. Our recommendations are:

1. Formal consultation with foreign carriers

Regulators must understand that aviation is a globally interconnected enterprise and must write security regulations that reflect this reality. Most often, new rules are written without industry input and review. This deprives the regulatory process of the operational insight and expertise the airline industry can provide. Greater collaboration would ensure more effective and more efficient security measures.

In the long-term, consultative public/private partnerships can define and promote a unifying security vision, which can be reflected in national policy. In the short-term, stakeholders can create "playbooks," which respond to threats to aviation proactively rather than reactively.

IATA believes that industry consultation must be regular, formal, and empowered. Collaboration must be tied into policy, which is then seamlessly tied into regulation. DHS has a stakeholder body known as the Sector Coordination Council (SCC), which attempts to provide a public/private partnership. However, it is neither integrated firmly into security policymaking nor does it include foreign representation. Rarely does the SCC process produce more efficient regulations or more refined national policies.

Finally, we believe other like-minded regulators could benefit from their own SCC-type national organizations. We believe ICAO is uniquely positioned to create a template for such organizations and to promulgate them internationally.

IATA recommends that DHS engage in formal and continuous consultation on aviation security matters with all air carriers through a cooperative and deliberative process. We are asking DHS to:

- Formally establish an international aviation workgroup under the DHS Aviation Security Advisory Committee (ASAC)
- Revitalize and empower the Sector Coordination Council (SCC) to play a definitive role in aviation security policymaking
- Allow foreign airlines, under the coordination of IATA, to join and participate as full members of the SCC

2. Refine existing TSA emergency orders to better address the international environment

Airlines operate across the globe under extremely different environments: laws, infrastructures, and cultural diversity should all be taken into account. Airlines have hands-on experience in these different environments. However, TSA imposes one-size-fits-all measures on international carriers, which often simply cannot be implemented in certain airports, countries or regions.

Moreover, although DHS is using risk management principles in targeting passengers from a list of 14 States for further screening, we believe the country "blacklist" approach is counter-productive. Our experience with blacklists in the safety field shows they can do more harm than good and can lead to diplomatic actions, such as retaliation. Instead, targeting people for screening should be based on the individual through the better use of passenger data. IATA recommends that DHS:

- Move toward risk-based and "performance-based" regulations, which would be flexible enough in their wording to allow carriers to make sure DHS's objective is reached in a way, which complies with local specificities
- Make better use of passenger data rather than subjecting passengers from whole States to enhanced screening
- Increase security focus on high-risk areas of the world instead of relying on one-size-fits-all directives.

3. Eliminate inefficiencies in the passenger data collection process

Under existing US regulation, carriers serving the US market are required to provide extensive data relating to all persons traveling on flights to, from and within the United States. Whether that information is provided to meet requirements for PNR access, APIS Quick Query (AQQ) or TSA's Secure Flight, the data provided is largely the same. We need the ability to transmit data in a consistent format to a single DHS portal.

As evidenced on December 25th, agencies failed to identify the potential threat, even with the provision of vast amounts of personal data at least 3 days before the flight. As indicated in the White House Review Summary to President Obama on January 7, 2009, this failure to "connect the dots" was primarily due to fragmentation within the United States Government and the inability to fully share information across agencies. We advocate deployment of more robust systems within DHS that better analyze and synthesize the data already transmitted to DHS's component agencies. IATA recommends:

- DHS collect a single set of information on each passenger from carriers that can be shared widely and seamlessly among DHS and intelligence agencies

4. Strengthen government-to-government outreach to harmonize and to coordinate on security issues

The US takes a different approach from most countries, because it mandates security procedures for incoming flights. The European Union, for instance, takes the stance that it can only regulate flights departing its territory.

The extraterritorial approach to security is problematic, mostly because US requirements can conflict with national norms. One example of this has been the 2005 US requirement for PNR data, which conflicted with EU data privacy directives. A similar example with today's situation is that in many countries, such as Germany, airlines are not allowed to perform physical screening on passengers. If a

government were to ask an airline to conduct such screening in Germany, that airline would be caught in the middle and placed in an impossible situation.

DHS should reach out to governments around the world before imposing new extraterritorial procedures on the airlines. One way to do this would be to make full use of ICAO's Aviation Security "Point of Contact" network. This would allow DHS and TSA to evaluate whether a new procedure is feasible at the world's airports. It would also increase the readiness of countries to assist airlines in complying with US requirements.

5. Over the longer term, focus on developing a next generation checkpoint

The December 2009 Detroit incident demonstrates that in the future aviation may need smarter and faster, next-generation passenger screening measures to confront new and emerging threats. While our current screening systems are serving us well, their underlying operational concepts and architecture are beginning to show their age, and they need to be replaced.

IATA is asking DHS to begin to look forward to field a new checkpoint. In the interim, we need to enhance the capabilities of the current system to extend its useable lifetime and increase its detection capabilities.

IATA recommends to the Department of Homeland Security (DHS) that this effort be accomplished in close cooperation and partnership with industry. Stakeholders at the highest level must develop an integrated vision and a road map for moving forward.

Principles of Next Generation Screening

The subject of today's hearing is, "An Assessment of Checkpoint Security: Are Our Airports Keeping Passengers Safe?" The short answer to this question is absolutely, "yes." The American public needs to understand that their security is the upmost concern of the airlines on which they fly and the airports in which they transit. Twenty four hours a day, three hundred sixty five days a year, professionals are standing watch to ensure their security. The procedures, processes, and

technology deployed since 9/11 have made this industry the most secure in its history.

Yet, those who would do us harm by injuring innocent passengers and by disrupting our economies are not standing still, and neither should our checkpoints. Today's checkpoint works and we are not advocating immediately discarding it for the next generation checkpoint. In fact, there is still service life left in these checkpoints. However, the day is rapidly approaching where the 40 year old concepts which serve as their underpinning will become obsolete. As Congress discusses novel drop-in technology for checkpoints, we believe it is essential to not mask the need for a new philosophy behind checkpoint architecture. For these reasons, we urge Congress to launch the process to build a next generation checkpoint capable and flexible enough to handle new and emerging threats to air transport.

We recommend that the next generation checkpoint be based on intelligence and supported by technology. Screening would consist of looking for bad people rather than bad things. We believe the volumes of passenger data currently collected by governments could be leveraged to make decisions about boarding pass issuance long before a passenger arrives at the airport. However, unlike today, the next generation checkpoint would require the US Government to:

- Align passenger data collections programs within DHS and between DHS and other Departments
- Screen passenger data more thoroughly against intelligence information and law enforcement data
- Develop a "red flag" system, which would objectively identify the level of screening a passenger would require before boarding

The next checkpoint should also rely on thorough and pervasive behavior detection. We believe highly trained behavior detection officers who question passengers and observe their mannerisms throughout the screening process would add a strong layer of detection. Tomorrow's checkpoint would enhance behavior detection by providing screeners with contextual background information on the traveler to assist in the questioning process. This type of intelligence based behavior detection would increase both the fidelity and also the objectivity of screening.

Screening technology supports intelligence in the next generation checkpoint by providing screeners with enhanced baseline methods for identifying explosives and firearms. This equipment would be in the primary screening lanes through which all passengers would quickly pass with little interruption. Additionally, the checkpoint would have enhanced lanes designed to inspect those passengers of whom little is known or of whom questions are raised, most likely at a slower rate with more fidelity.

The system described here envisions security for tomorrow's passenger as a road bump in the journey rather than a mountain. We believe the components of this checkpoint are available, but they require the will to be assembled and delivered to our airports.

Security and technology are often confused. IATA remains concerned that novel technology is being viewed as the silver bullet for the future. However, there is no silver bullet in security. For every technology with exciting detection capabilities there are complementary vulnerabilities, which can be open to exploitation. We urge this Subcommittee to challenge technology advocates to fairly assess capabilities against vulnerabilities.

Finally, we must not overlook the process through which technology moves from the laboratory to the airport. Fundamentally, the journey takes too long, and it is tainted by changing regulatory requirements, often producing a product which doesn't work in the real world.

Promising technology needs to pass the O'Hare test before it leaves the lab: it must perform its functions reliably and accurately under the same passenger load it would experience at O'Hare the day before Christmas. Perhaps such a test would have kept the explosive puffers purchased by the TSA out of long-term storage.

Conclusion

The security and safety of the flying public is the top priority of IATA and the aviation industry as a whole. The procedures, processes, and technology deployed since 9/11

have made this industry more secure than ever before. However, there is a clear need for continued vigilance and constant revision to ensure an even more secure future. Regulators worldwide must focus on improving intelligence communication and passenger screening programs in order to stay one step ahead of those whom would wish harm on our passengers.

As the Subcommittee reviews the events post-December 25th, we expect many will seek short-term fixes to security checkpoints. However, new technology cannot guarantee better security, cannot detect bad people, and is not the only solution for the future. Any new equipment must be fully vetted in the operational environment and justified in fulfilling a clear need and producing a clear enhancement at the checkpoint. Overall, we urge Congress to promote long-term improvements to intelligence coordination, to interdepartmental cooperation, and to security checkpoints in order to achieve the highest level of security for the flying public.